Attorney's Docket No. 1032326-000132

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	**MAIL STOP AF**
Christophe Clavier et al.	Group Art Unit: 2131
Application No.: 09/807,607	Examiner: Kaveh Abrishamkar
Filed: June 1, 2001	Confirmation No.: 2078
For: COUNTERMEASURE METHOD IN AN ELECTRONIC COMPONENT USING A SECRET KEY CRYPTOGRAPHIC ALGORITHM	

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants request review of the final rejection of claims 1-10 and 13-16 in the Office Action dated August 28, 2006. No amendments are being filed with this request.

This request is being filed with a Notice of Appeal.

The subject application contains two independent claims, 1 and 13. For the sake of brevity, this request will focus upon the issues presented by these two claims.

The claims are directed to countermeasures against external attacks that monitor cryptographic operations for the purpose of discovering secret information, such as keys that are used during the operations. An exemplary embodiment of the countermeasure is described with reference to the DES cryptographic algorithm. This algorithm comprises 16 computation rounds, which are respectively depicted in Figures 7-8 by the labels T1-T16.

Claim 1 recites a countermeasure method that includes the step of executing a first set of instructions in a cryptographic algorithm with a first manipulating means to deliver output data on the basis of input data. Referring to Figure 7, an example of this step is depicted in computation round T2, where the SBOX operation is executed with a first manipulating means that is implemented with a constants table TC_0. An example of such a table is illustrated in Figure 6. The table receives a 6-bit input signal b1...b6, and produces a 4-bit output signal a1...a4.

Claim 1 recites the further step of executing another set of instructions "with other manipulating means that are derived from said first manipulating means by complementation of at least one of said input data and said output data." Referring again to Figure 7, during computation round T1, the SBOX operation is carried out with the constants table TC_1. An

example of this table is illustrated in Figure 9. As can be seen, the output values a1...a4 in this table are the complements of the output values that are delivered by the table TC_0.

The rejection of claim 1 is based upon a combination of the Kocher et al. and Chow et al. patents. In rejecting the claim, the Office Action refers to Figures 1 and 2 of the Kocher patent, as well as column 1, line 66 to column 2, line 24, as disclosing the steps of executing the first set of instructions with the first manipulating means and executing another set of instructions with other manipulating means that are derived from the first manipulating means. As pointed out in the paragraph bridging pages 1 and 2 of Applicants' response filed June 21, 2006, it is not apparent how these portions of the patent are being interpreted to disclose the claimed subject matter. In response to the Applicants' request, the final Office Action states that the initial permutations illustrated in Figure 1 of the Kocher patent are being interpreted as the claimed first manipulating means, and the other manipulating means are the subkeys.

The record is still unclear as to how the disclosure of the Kocher patent is being correlated with the recitations of the claim. On one hand, the Examiner appears to be stating that the permutation operations constitute the manipulating means. However, the Kocher patent does not discloses that a permutation operation that is performed during step 145, for example, is derived from the permutation operation that is performed at step 120. It does not disclose whether the same permutation, i.e. re-ordering of bits, or a different permutation occurs. Thus, it is unclear whether the same "manipulation means" or different respective manipulation means are employed during the different steps.

On the other hand, the Examiner might be relying upon the keys, per se, as being the manipulating means, since the subkeys are derived from the initial key. In that case, it is not clear how a key can be considered to be a manipulating means of the type recited in the claim. A key does not have input data or output data associated with it. It is simply a string of bits. There is no "manipulating" of data that occurs in a key.

Thus, the record remains unclear on the manner in which the Kocher patent is being interpreted to suggest the claimed steps of executing first and second sets of instructions with respective manipulating means, where one manipulating means is derived from the other. For this reason alone, the application is not ripe for appeal.

Claim 1 recites that the step of executing the first set of instructions with a first manipulating means delivers output data on the basis of input data. The claim further recites that the derivation of the other manipulating means from the first manipulating means occurs "by complementation of at least one of said input data and said output data." The Office Action acknowledges that one manipulating means of the Kocher patent (however it is being

interpreted) is not derived from another manipulating means through complementation of input or output data. To this end, therefore, it refers to the Chow patent, particularly at column 18, line 50 to column 19, line 13, as well as column 20, line 28.

The Chow patent is concerned with prevention of a user's ability to modify computer software to override built-in controls (column 3, lines 13-16). To accomplish this objective, the patent discloses a technique for *recoding* software, so that it is fragile to tampering (column 5, lines 8-9, and column 9, lines 12-14). Recoding is accomplished by mapping each variable in the software to a new set of variables that cannot be easily traced back to the original variables. (Column 11, lines 8-11). The patent discloses that this technique is also useful for hiding DES keys (column 20, lines 28-29). This portion of the patent goes on to explain one example in which two of the disclosed techniques for hiding variables, namely Bit-Exploded and Bit-Tabulated coding are employed to hide the DES key. As stated in step 2 at column 21, lines 4-5, when this technique is employed "the key has now completely disappeared".

The Office Action does not establish how the teachings of the Chow patent could be applied to the cryptographic process of the Kocher patent in a manner that would result in the subject matter of claim 1. The claim recites that a first set of instructions are executed with a first manipulating means, and the second set of instructions are executed with other manipulating means "that are derived from said first manipulating means by complementation of at least one of said input data and said output data." As noted above, the Office Action does not identify what is considered to the input data and output data of the Kocher patent that is used to derive one manipulating means from another. Furthermore, there is no disclosure in the Chow patent which suggests that one of the input data or output data associated with one manipulating means, that is employed during the execution of the first set of instructions, can be complemented to derive another manipulating means that is employed during the second set of instructions. To the extent that the Chow patent discloses complementation, it is only for the purpose of *hiding* one set of data, by replacing it with another set of data. There is no disclosure that a complementation function should be employed to derive two different types of manipulating means that are respectively employed during the execution of different sets of instructions.

The Office Action simply does not explain how any possible application of the Chow disclosure to the Kocher process would result in the claimed subject matter.

Claim 13 recites an electronic component that provides countermeasures against attacks. This component has, among other elements, a processor that executes instructions in a cryptographic algorithm, in accordance with a selected one of a plurality of different

manipulating means stored in a program memory. The claim further recites "means for generating a random value for selecting the manipulating means to be employed during a given execution of said algorithm". Thus, the random value is used to select one of the pluralities of different manipulating means stored in the memory.

In responding to Applicants' traversing the rejection of this claim, the final Office Action refers to the Chow patent at column 19, lines 60-64. This passage states that "the positions of the bits in the index and the result of the above lookup can be random... so the encoding chosen for the data is not exposed." The Office Action apparently points to this passage because it contains the word "random". However, the randomness that is discussed in this passage does not relate to the selection of different ones of stored manipulating means for a given execution of an algorithm. The randomness of the positions of bits in an index for a lookup table has nothing to do with the claimed subject matter.

The Office Action does not explain how this disclosure leads a person of ordinary skill in the art to the claimed subject matter. For the sake of argument, even if the different subkeys in the Kocher patent are considered to be different manipulating means, there is no disclosure in the Chow patent suggesting that one of the plurality of subkeys is randomly selected for a given round of the DES algorithm.

Accordingly, the Office Action does not establish that the Chow patent renders obvious the differences between the Kocher patent and the subject matter recited in claim 13.

For at least the foregoing reasons, the final Office Action does not establish a record that would form a proper basis for going forward with an appeal. It does not show that all of the limitations of the independent claims are taught or suggested by the prior art references, even when they are considered in combination with one another. Withdrawal of the final Office Action is respectfully submitted to be in order.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: February 28, 2007

By: _____
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620